

Centenas de supermercados perderam o frio em uma noite, e o descongelamento veio de função legítima

Na noite de domingo, 11 de outubro, alguém colocou em descongelamento os controladores de refrigeração de centenas de supermercados na França, com a comida dentro. O ciclo normal de uma hora foi esticado para oito, o que atrasou o alarme que avisaria a loja. A temperatura chegou perto de 50 graus em muitas lojas. Houve equipamento pegando fogo e aspersor disparando. Nenhum grupo assumiu, nenhum resgate foi pedido, e a interface de administração do controlador estava na internet.

Alerta CERTFR-2026-ALE-012 · Danfoss AK-SM e AK-SC, Copeland e Dixell XWEB · CVE-2025-41450, 41451 e 41452 · Pelo menos 4.500 interfaces visíveis · Leitura: cadeia de frio

Por que esta análise: o ataque de 11 de outubro não usou falha nova nem ferramenta sofisticada. Usou equipamento de automação predial exposto na internet, firmware antigo, credencial que o operador não controla e uma função de descongelamento que existe para ser usada. É o padrão que se repete em medidor de combustível, controlador de água e sistema de ar condicionado, e é o padrão que a maior parte do varejo brasileiro tem instalado hoje sem inventário.

O que você leva daqui: a cadeia de exploração publicada em agosto e por que ela é fácil; a aritmética de exposição, que aumentou depois do alerta; a ordem correta das medidas do CERT-FR, incluindo a cláusula de seguro que quase ninguém checa antes de cortar acesso; o que a detecção precisa correlacionar quando o atacante usa função legítima; e três evidências que um conselho pode exigir ainda nesta semana de quem opera cadeia de frio.

A reconstrução pública converge em poucos fatos e divergem nos números. O ataque começou na noite de domingo, 11 de outubro, e apareceu na manhã de segunda, quando as lojas abriram. Os controladores de refrigeração foram colocados em descongelamento forçado, com a mercadoria dentro. A temperatura subiu até cerca de 50 graus em muitas lojas depois de algumas horas. Houve equipamento pegando fogo e aspersor de incêndio disparando, o que somou dano de água ao prejuízo de mercadoria.

A contagem de lojas depende de quem conta. Intermarché e Netto, do grupo Les Mousquetaires, falam em pelo menos 300 lojas pela AFP e cerca de 150 pela Reuters. A Coopérative U reportou entre 80 e mais de 100 de um parque de 2 mil, com a cadeia de frio aguentando na maioria. Carrefour citou 80 supermercados, Monoprix cerca de 5% de suas aproximadamente 490 lojas, e o E.Leclerc falou em várias, por meio de um fornecedor de refrigeração que não nomeou. A Reuters trabalha com um piso de 350 supermercados. O presidente do Intermarché disse à BFM TV que a perda pode chegar a dezenas de milhões de euros em um único dia.

A parte que não foi ataque, foi uso

Descongelamento programado é operação de rotina em refrigeração comercial. O equipamento existe para fazer isso. O que foi manipulado é o quando, o por quanto tempo e o quanto.

O detalhe que a Nozomi Networks destacou é o que transforma o episódio em caso de estudo: o ciclo de descongelamento foi estendido de uma hora para oito. Isso não é só mais dano, é menos alarme. O alarme de temperatura alta de um sistema de refrigeração dispara em desvio sustentado fora da janela esperada. Dentro de

uma janela de descongelamento declarada como legítima, a temperatura subindo é o comportamento previsto. A loja estava fechada, não havia gente para sentir calor no corredor, e o sinal que deveria acordar alguém estava suprimido pela própria configuração.

Vale fixar a consequência para quem monta detecção. Não havia malware para assinatura pegar, não havia arquivo cifrado, não havia processo estranho rodando. Havia escrita de configuração em horário incomum, feita por uma sessão autenticada.

A cadeia de exploração estava publicada desde agosto

A Team82, da Claroty, divulgou em agosto três falhas na interface web da linha AK-SM 800A da Danfoss. Nem o CERT-FR nem a Danfoss confirmaram qual caminho foi usado no ataque, e essa ressalva é importante. Mas a cadeia publicada explica por que a barreira era baixa.

A CVE-2025-41450 é um caminho de autenticação escondido que aceita uma senha derivada da data corrente do próprio equipamento, o chamado código do dia. É um mecanismo de suporte de fábrica, o tipo de atalho que existe para o técnico entrar quando o cliente perdeu a senha. Corrigida na R4.2. A CVE-2025-41451 é injeção de comando no campo de senha da configuração de alarme por e-mail, o que dá execução de código depois de autenticado. A CVE-2025-41452 permite a um usuário autenticado injetar diretivas de Nginx substituindo o arquivo de cabeçalhos, com manipulação de tráfego ou negação de serviço. As duas últimas foram corrigidas na 4.3.1.

Junte as duas primeiras e o resultado é execução de comando contra um equipamento alcançável pela internet, sem credencial válida, por um caminho que o operador não sabia que existia. Existe hoje um kit público, o FROMAGEGATE, com prova de conceito, emulador e regras de Suricata e Sigma. A ressalva do próprio autor merece registro: a Claroty omitiu o algoritmo real do código do dia, então a prova de conceito não funciona contra firmware de verdade e as assinaturas precisam ser ajustadas com tráfego real. O valor do kit, hoje, está na detecção, não na exploração.

O parque que ninguém ia trocar

Aqui está o nó que nenhuma recomendação de atualizar firmware resolve. A Danfoss diz que a maioria dos equipamentos atingidos é da linha AK-SM 800 ou AK-SC 355, classificada como legado, sem atualização de software ou de segurança, e que a empresa vinha recomendando migração há tempo. O restante é AK-SM 800A da geração atual rodando firmware antigo. O alerta do CERT-FR estende a lista para Copeland XWEB e Dixell XWEB, acrescentados em 13 de outubro.

Equipamento de refrigeração comercial tem vida útil medida em quinze anos ou mais, é instalado dentro de obra civil e entra no orçamento de ativo imobilizado, não no de tecnologia. O controlador é um acessório barato de um equipamento caro. Nessa contabilidade, trocar o controlador porque o fabricante encerrou o suporte de segurança nunca ganha a disputa por capital. É a mesma lógica que mantém no ar inversor solar, elevador, nobreak e central de ar condicionado com software de uma década atrás.

A aritmética da exposição piorou depois do alerta

Em 12 de outubro, um pesquisador contou 2.752 sistemas Danfoss expostos, dos quais 1.590 na França. No dia seguinte, a Reuters localizou pelo menos 4.500 interfaces visíveis pelo Shodan. A Onyphe verificou que só uma pequena minoria rodava a versão mais recente. A Claroty já havia relatado, antes do ataque, milhares de interfaces de gerenciamento da linha AK-SM 800A alcançáveis pela internet.

O número subir entre um dia e outro diz mais sobre a varredura do que sobre novas instalações, mas o recado prático é o mesmo: alerta público não derruba exposição sozinho. Há um contraponto útil no mesmo levantamento da Nozomi. No setor de combustível, a exposição de medidores de tanque caiu cerca de 56% entre março e junho deste ano, depois de aviso setorial e resposta coordenada. Dá para reduzir. Precisa de alguém com nome e prazo.

As medidas do CERT-FR, na ordem em que ele manda fazer

Para quem não foi comprometido, são quatro passos. Primeiro, tirar a exposição à internet de qualquer unidade afetada e de qualquer unidade com IP público. Segundo, revisar a configuração inteira, com atenção especial à programação de descongelamento. Terceiro, devolver o acesso só por VPN segura ou rede protegida, tratando filtro de IP de origem do prestador como medida temporária, nunca definitiva. Quarto, aplicar as boas práticas do fabricante: atualizar firmware, pôr o nível de segurança em Strict e trocar senha padrão.

Para quem foi comprometido, entram mais dois: reiniciar o equipamento, ou restaurar para configuração de fábrica se o reinício não bastar, e reconfigurar antes de devolver ao serviço. O alerta é explícito num ponto que costuma ser mal lido: restauração de fábrica remove persistência e não remove vulnerabilidade, então equipamento resetado e religado na internet é equipamento reinfectado. O CERT-FR também avisa que as campanhas provavelmente continuam.

No meio do primeiro passo há a recomendação mais incomum do documento, e vale ler duas vezes: checar as condições do seguro antes de cortar o enlace de dados com a empresa de refrigeração. Contrato de manutenção, e a cobertura de perda de mercadoria atrelada a ele, costuma exigir telemetria contínua chegando ao prestador. Cortar o acesso sem olhar a cláusula fecha o problema técnico e abre o de responsabilidade.

O que a detecção precisa correlacionar

Como o atacante usa função legítima com sessão autenticada, a telemetria que importa não é de ameaça, é de operação. Quatro sinais, cruzados entre si, cobrem o caso: mudança de ponto de ajuste de temperatura; ciclo de descongelamento com duração fora do padrão da loja; login remoto novo, de origem ou horário incomum; e escrita de configuração, especialmente em programação e em parâmetro de alarme.

O valor está no cruzamento. Mudança de ponto de ajuste sozinha é rotina de técnico. Mudança de ponto de ajuste às três da manhã, de um IP que nunca apareceu, seguida de ciclo de descongelamento três vezes mais longo que a média daquela loja, é incidente. Nenhum desses eventos precisa de sensor novo: eles já existem no histórico do próprio supervisor de refrigeração, que quase nunca é lido por quem cuida de segurança.

O que muda para quem opera no Brasil

A exposição direta ao parque Danfoss, Copeland e Dixell aqui não foi medida publicamente, e seria leviano inventar número. O que dá para afirmar é que são marcas correntes em refrigeração comercial brasileira, presentes em supermercado, centro de distribuição, frigorífico, farmácia, laboratório e hospital, e que o modelo de operação é o mesmo: manutenção terceirizada com acesso remoto, muitas vezes por modem celular instalado pela própria empresa de refrigeração, sem passar pela rede corporativa nem pelo inventário de TI.

Esse é o ponto cego que importa. Em boa parte das operações, quem contratou o acesso remoto foi a área de manutenção predial ou de engenharia, não a de tecnologia, e o levantamento de ativo de segurança nunca chegou lá. Vale fazer a pergunta direta nesta semana: existe modem, roteador ou IP público instalado pela empresa de refrigeração dentro das suas lojas, e quem sabe dizer quantos são?

A diferença brasileira mais séria está em quem guarda produto termossensível com obrigação regulatória de registro de temperatura. Farmácia, distribuidora de medicamento, laboratório e serviço de saúde operam sob exigência de controle e registro contínuo de temperatura de armazenamento, e esse registro é feito pelo mesmo supervisor que foi atacado na França. Perda de mercadoria é prejuízo. Perda de integridade do registro de temperatura de medicamento ou de imunobiológico é problema sanitário e de rastreabilidade, com consequência regulatória e com impossibilidade prática de provar que o lote ficou dentro da faixa. Quem tem esse perfil deveria tratar o registro de temperatura como evidência, com cópia fora do equipamento que o gera.

Leitura LATAMSEC

O ataque de 11 de outubro vai ser citado como caso de OT, e é. Mas o que ele mostra de novo não é técnico. É de governança de ativo: existe uma classe de equipamento que tem endereço na internet, software desatualizado,

credencial que o dono não controla, fornecedor com acesso permanente e nenhum responsável nomeado dentro da empresa. Chamar isso de risco cibernético atrasa a conversa, porque joga o problema para um time que não tem mandato sobre o ativo. É risco operacional com vetor digital, e o dono é quem responde pela operação da loja.

Três evidências que um conselho pode pedir, com prazo, sem precisar entender de refrigeração:

- Inventário com nome e número. Quantos controladores de refrigeração existem, de quais fabricantes e versões, quantos têm IP público ou modem celular próprio, e qual deles está fora do suporte de segurança do fabricante. Prazo de duas semanas. Se a resposta vier sem número, essa é a resposta.
- Cláusula de acesso remoto do contrato de manutenção. Como o prestador entra, com qual credencial, se é individual ou compartilhada, se há segundo fator, quem revoga quando o técnico sai da empresa dele, e qual a obrigação contratual dele de manter firmware atualizado. Junto com isso, a leitura da apólice sobre exigência de telemetria contínua.
- Prova de que o registro de temperatura sobrevive ao equipamento. Para quem tem obrigação sanitária, demonstrar que o histórico de temperatura é copiado para fora do supervisor de refrigeração e que uma restauração de fábrica do controlador não apaga a evidência do lote.

A última observação é de calendário. O CERT-FR diz que as campanhas provavelmente seguem ativas, a exposição medida não caiu nos primeiros dias e existe kit público de detecção disponível. A janela para fazer isso sem pressa já é curta.

Pontos de atenção da semana

MECANISMO

O ataque usou a função que o equipamento existe para executar

Descongelamento programado é operação normal de refrigeração comercial. O que foi anormal é o horário, a duração e o ajuste de temperatura. Esticar o ciclo de uma para oito horas serviu justamente para não acionar o alarme de temperatura alta, que dispara em desvio sustentado. Não houve malware, não houve criptografia de arquivo, não houve nada que um antivírus de endpoint pudesse ver.

EXPOSIÇÃO

A conta de interfaces visíveis cresceu depois do ataque, não diminuiu

Em 12 de outubro, um pesquisador contava 2.752 sistemas Danfoss expostos, 1.590 deles na França. Um dia depois, a Reuters achou pelo menos 4.500 interfaces visíveis pelo Shodan. A Onyphe apurou que só uma pequena minoria rodava a versão mais recente do software. O alerta público não derrubou a exposição nos primeiros dias.

FIM DE VIDA

Boa parte do parque atingido não tem correção para aplicar

A Danfoss diz que a maioria dos equipamentos afetados é da linha AK-SM 800 ou AK-SC 355, classificada como legado e sem atualização de software ou de segurança, ou AK-SM 800A da geração atual rodando firmware antigo. Onde não existe patch, a única defesa é isolamento, controle compensatório ou troca do equipamento, e nenhuma das três cabe em um ciclo de atualização.

CONTRATO

O CERT-FR manda checar a apólice antes de cortar o enlace da manutenção

É a recomendação mais incomum do alerta e a mais prática. Muito contrato de manutenção de refrigeração, e a cobertura de seguro atrelada a ele, exige telemetria contínua chegando à empresa que faz a manutenção. Cortar o acesso sem olhar a cláusula resolve o problema de segurança e abre um problema de responsabilidade por perda de mercadoria.

ALCANCE

A França foi onde doeu, mas não foi o único país com o mesmo parque

Felix Aimé, da Sekoia, relatou à Reuters que Espanha, Portugal, Polônia, Alemanha e Bélgica também foram afetadas. A ANSSI acionou agências europeias e o Ministério Público de Paris abriu inquérito pela seção de cibercrime, delegado ao escritório anticiber, para contar vítimas e ligar o ataque às perdas.

Fontes

CERT-FR · CERTFR-2026-ALE-012: Compromissions de contrôleurs distants de systèmes de réfrigération, com a lista de equipamentos atingidos, as medidas em ordem para quem não foi comprometido e para quem foi, e o aviso de que restauração de fábrica sozinha não basta.

<https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-012>

Nozomi Networks · French Supermarket Fridge Cyberattacks and the Risks of Internet-Connected OT, com o ciclo de descongelamento esticado de uma para oito horas, as três CVE da Team82, as contagens de exposição e o precedente dos medidores de combustível.

<https://www.nozominetworks.com/blog/french-supermarket-fridge-cyberattacks-and-the-risks-of-internet-connected-ot>

Al Jazeera · Hundreds of supermarkets in France hit by 'unprecedented' cyberattack, com a contagem de lojas por rede, a estimativa de perda do Intermarché, o pedido de transparência da federação de varejo e o alcance europeu relatado pela Sekoia.

<https://www.aljazeera.com/news/2026/10/13/unprecedented-cyberattack-hits-french-supermarkets-causing-food-losses>

Facilities Dive · Hack of Danfoss refrigeration controllers in Europe causes tens of millions in food losses, com a declaração da Danfoss sobre equipamento legado, o aviso anterior da CISA e os números da Armis sobre falha explorada e protocolo inseguro em sistema predial.

<https://www.facilitiesdive.com/news/hack-of-danfoss-refrigeration-controllers-in-europe-causes-tens-of-millions/832832/>

FROMAGEGATE · PoC e kit de detecção para CVE-2025-41450, 41451 e 41452, com a cadeia das três falhas, as regras Suricata e Sigma, o emulador para teste e a ressalva de que o algoritmo real do código do dia foi omitido pela Claroty.

<https://github.com/msuiche/fromagegate>

Publicado em latamsec.com.br/recursos/controladores-refrigeracao-expostos-varejo/ · 19 de outubro de 2026